COMUNE DI MANFREDONIA

INDICAZIONI OPERATIVE PER LA REDAZIONE DELLA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI (DPIA)

in attuazione del Regolamento UE 679/2016 ("GDPR")

ex artt.35 e 36

SOMMARIO

CONTESTO DI RIFERIMENTO

L'introduzione è necessaria al fine di inquadrare sotto un profilo contestuale il Regolamento Europeo 679/2016 (General Data Protection Regulation meglio noto come "GDPR"), entrato in vigore il 24 maggio 2016 ma pienamente applicabile a partire dal 25 maggio 2018, che uniforma e armonizzare (anche con l'entrata in vigore del D.Lgs. 101/2018) le legislazioni dei Paesi Europei con riguardo alla materia di protezione dei dati personali. L'esigenza di una rivisitazione della normativa in materia di protezione dei dati personali si apprezza in relazione al mutato contesto politico, economico e sociale di riferimento del tutto differente rispetto a quello passato; ciò è dato dallo sviluppo repentino delle moderne tecnologie (in primis mobile devices, smartphone, tablet, social network, ecc.; in seconda battuta strumenti Internet Of Things, sistemi di Data Analytics e Big Data, Business Intelligence, ecc.), grazie alle quali è pensabile e apprezzabile anche il valore economico del dato.

PREMESSA

Oggetto e obiettivo del documento

A partire dal 25 maggio 2018, tutti i Titolari del trattamento – pubblici e privati – devono applicare quanto previsto dagli articoli 35 e 36 del GDPR relativamente agli aspetti di Valutazione d'Impatto sulla Protezione dei Dati (c.d. "DPIA") e Consultazione preventiva.

Una DPIA è un processo volto a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, analizzando detti rischi e determinando le misure necessarie per affrontarli. Le Valutazioni d'Impatto sulla Protezione dei Dati sono strumenti importanti per la responsabilizzazione, in quanto sostengono i Titolari del trattamento non soltanto nel rispetto dei requisiti del GDPR, ma anche al fine di dimostrare che sono state adottate misure appropriate per garantire il rispetto dello stesso regolamento (cfr. articolo 24). In altre parole, una DPIA è un processo volto a garantire e dimostrare la conformità ed in generale il principio di "***Accountability***".

Inoltre, laddove una Valutazione d'Impatto riveli la presenza di rischi residui elevati, il Titolare del trattamento sarà tenuto a richiedere la Consultazione preventiva dell'autorità di controllo in relazione al trattamento (articolo 36, paragrafo 1 del GDPR).

Il presente documento di indirizzo tiene quindi conto di quanto previsto dalla normativa di riferimento citata, ma resta comunque soggetto a possibili futuri aggiornamenti sulla base di eventuali interventi in materia da parte dell'Autorità Garante.

Ambito di applicazione del documento

Il presente documento ha lo scopo di fornire indicazioni utili in grado di coadiuvare il Titolare, nella più veloce e completa definizione, di un processo - e relative procedure - per la gestione di tutte le attività sottostanti gli aspetti di Data Protection Impact Assessment (sinteticamente DPIA). Ai sensi dell'art. 35 par. 1 si definisce che:

"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, ***prima*** *di procedere al trattamento, una Valutazione dell'Impatto dei trattamenti previsti sulla protezione dei dati personali".*

Quindi, l'applicazione di un processo DPIA diventa obbligatoria tutte le volte che ci troviamo in presenza di un trattamento che comporti un rischio elevato per i diritti e le libertà delle persone fisiche.

Per poter inquadrare meglio l'obbligatorietà dell'applicazione di un processo DPIA si può fare riferimento a quanto espresso dalla linea guida WP248 17/IT Gruppo Articolo 29, ora sostituito dall'EDPB – consultabili al link: http://www.interlex.it/2testi/autorit/wp248dpia.pdf), che riportano le principali casistiche di trattamenti che possono comportare un rischio elevato per i diritti e le libertà delle persone fisiche, ovvero:

- Profilazione degli interessati
- Realizzazione di valutazioni automatiche con effetti legali o comunque significativi
- Monitoraggio sistematico degli interessati
- Trattamento dati sensibili (ora categorie particolari di dati personali, art. 9 GDPR)
- Elaborazione di dati su larga scala utilizzando più fonti di dati di origine diversa
- Uso di nuove tecnologie o soluzioni organizzative
- Trasferimento dati oltre i confini UE
- Trattamenti che impediscono all'interessato di esercitare un proprio diritto o l'uso di un servizio o l'attivazione di un contratto.

Le presenti indicazioni si applicano quindi in tutti i casi in cui il COMUNE DI MANFREDONIA si dovesse trovare a valutare trattamenti che in qualche maniera ricadono nell'ambito delle categorie sopra citate o che comunque in generale possono presentare, anche potenzialmente, rischi elevati.

QUADRO NORMATIVO

→ REGOLAMENTO EUROPEO 679/2016 - GDPR

→ Considerando C84, C89, C90, C91, C92, C93, C94, C95 GDPR

→ WP248 - Linee guida in materia di Valutazione d'Impatto sulla Protezione dei Dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del GDPR

Definizioni normative di riferimento

Anonimizzazione: tecnica di trattamento dei dati personali tramite la quale i dati personali non possano più essere attribuiti a un interessato specifico, nemmeno attraverso l'utilizzo di informazioni aggiuntive.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Autorità di controllo: è l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Cifratura: tecnica di trattamento dei dati personali tramite la quale i dati personali vengono resi non intellegibili a soggetti non autorizzati ad accedervi.

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Contitolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri determina le finalità e i mezzi di trattamento dei dati personali;

Data Breach: è un incidente di sicurezza in cui i dati personali vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato o persi accidentalmente.

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati biometrici: i dati ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

DPIA: acronimo di Data Protection Impact Assessment (Valutazione di Impatto sulla Protezione dei Dati).

Interessato: persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

Misure di sicurezza: misure tecniche ed organizzative adeguate a garantire un livello di sicurezza dei dati trattati adeguato al rischio.

Nuovo trattamento: trattamento di dati personali che comporta l'utilizzo di nuove tecnologie o è di nuovo tipo e in relazione al quale il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.

Privacy by-Design / Privacy by-Default: l'incorporazione della privacy a partire dalla progettazione di un processo aziendale, con le relative applicazioni informatiche di supporto. La prima introduce la protezione dei dati fin dalla progettazione per caso specifico, la seconda per impostazione predefinita di una pluralità di casi tra loro omogenei.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi,

l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del regolamento;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Sub responsabile: persona fisica o giuridica designata dal responsabile del trattamento previa autorizzazione scritta del titolare del trattamento;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare o suo delegato del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Titolare del trattamento o suo Delegato/Designato: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Adempimenti prescritti dalla normativa

Ai sensi dell'art 35 del GDPR "Valutazione d'impatto sulla protezione dei dati":

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il Responsabile della Protezione dei Dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione. 4.5.2016 L 119/53 Gazzetta ufficiale dell'Unione europea IT

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Ai sensi dell'art 36 del GDPR "Consultazione preventiva":

1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:

a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le finalità e i mezzi del trattamento previsto;

c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;

d) ove applicabile, i dati di contatto del titolare della protezione dei dati;

e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;

f) ogni altra informazione richiesta dall'autorità di controllo.

4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.

5. Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

In capo al COMUNE DI MANFREDONIA, in caso di nuovi trattamenti o durante la revisione dei trattamenti esistenti vige:

A) Obbligo di redigere una DPIA quando questi possono presentare un rischio elevato per i diritti e le libertà delle persone.

Si evidenzia quindi che la redazione di un DPIA è obbligatoria quando vi è :

- un trattamento con un rischio probabile per i diritti e le libertà delle persone fisiche.

Nello specifico: Il Titolare deve valutare preventivamente la potenzialità del rischio del trattamento tenendo in considerazione alcune informazioni che gli devono consentire di decidere se procedere o meno alla realizzazione della DPIA, nello specifico occorre almeno valutare:

- gli strumenti tecnologici, in modo particolare quelli nuovi
- la natura del trattamento
- I dati oggetto del trattamento
- Il contesto e le finalità del trattamento.

Occorre inoltre tenere presente che alcuni trattamenti sono esclusi dalla obbligatorietà della valutazione di impatto:

- trattamenti esenti secondo gli elenchi forniti dall'autorità di controllo
- Particolari trattamenti leciti fra cui
  - o il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, par. 1, lett. c);
  - o il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1, lett. e)

B) Obbligo di consultare l'autorità di controllo (prima di procedere al trattamento) qualora la valutazione d'impatto indichi la presenza di un rischio elevato nel trattamento in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

Nello specifico: tale obbligo è previsto se si ritiene che il trattamento sottoposto a DPIA violi il regolamento GDPR, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio.

C) Obbligo di consultare l'autorità di controllo (prima di procedere al trattamento) in relazione al trattamento per l'esecuzione di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

Soggetti attivi

I soggetti attivi sono tutti coloro che si occupano, sin dalla fase di raccolta delle informazioni, dei trattamenti del processo e della procedura di DPIA.

RUOLI COINVOLTI

RUOLO AZIENDALE	RESPONSABILITÀ PRINCIPALI NEL PROCESSO DI DPIA
Titolare del trattamento	• Delega la responsabilità sul processo di DPIA e l'eventuale consultazione preventiva (quando necessaria) • Fornisce le risorse organizzative e finanziarie affinché sia possibile la realizzazione del processo di DPIA ed i conseguenti adeguamenti normativi e di sicurezza.
Responsabile del processo a cui afferisce il trattamento (Designato/Delegato al trattamento)	• Coordina le attività necessarie alla DPIA per i nuovi trattamenti ed è responsabile della verifica della implementazione delle misure di sicurezza necessarie. • È responsabile della raccolta delle informazioni sul trattamento per le verifiche preventive • È responsabile delle verifiche preventive di conformità del trattamento • Coadiuva il DPO nelle verifiche preventive sull'obbligatorietà della esecuzione di una DPIA • In caso di un trattamento esistente che presenta un cambiamento del profilo di rischio coordina le attività per l'aggiornamento della DPIA • Implementa la strategia nella gestione del trattamento • Segnala al Titolare e al DPO il nuovo trattamento e/o la modifica di un servizio esistente • Partecipa alla valorizzazione degli impatti e probabilità per le minacce individuate • Assiste il DPO nella Consultazione Preventiva
Amministratore di Sistema / Referente o figura simile	• Supporta il processo di DPIA fornendo competenze ed informazioni relativamente agli aspetti tecnici di competenza • Partecipa alla valorizzazione degli impatti e probabilità per le minacce ICT individuate • Implementa le modifiche richieste in termini di soluzioni di sicurezza

Referente interno / Consulente Privacy (Privacy Officer)	• Descrive e documenta il trattamento in tutte le sue caratteristiche • Collabora con il Titolare, il Designato e il DPO nella Valutazione dell'Impatto • Assiste il Designato e il DPO nelle verifiche preventive (conformità e necessità DPIA) • Assiste il Designato e il DPO nel garantire il rispetto degli obblighi diDPIA, tenendo conto della natura del trattamento e delle informazioni a loro disposizione. • Nel caso in cui il trattamento preveda l'impiego di Sistemi Informatici esterni, si confronta con i Responsabili del trattamento chefornisconо il servizio. • Supervisiona l'implementazione delle misure di sicurezza necessarie. • Partecipa alla valorizzazione degli impatti e probabilità per le minacce individuate • Collabora con il DPO nel processo di Consultazione Preventiva.
DPO	• Assiste il Designato e gli altri soggetti coinvolti nella definizione della Strategia e nello svolgimento della DPIA, monitora lo svolgimento, verifica se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR. • È Responsabile della verifica di obbligatorietà della DPIA • Coadiuva il Designato e gli altri soggetti coinvolti nella verifica preventiva di conformità del trattamento • È responsabile del processo di consultazione preventiva e fungere da interfaccia per l'Autorità di Controllo.

CONTENUTI ED INTERAZIONI DEL PROCESSO DPIA

Che cosa è la DPIA e a che cosa serve

Il Data Protection Impact Assessment (DPIA) è un processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo. Il DPIA va inquadrato come uno strumento essenziale e fondamentale per tutti i titolari e responsabili del trattamento al fine di dar corso al nuovo approccio alla protezione dei dati personali richiamato dal regolamento europeo e fortemente basato sul principio della accountability.

Un processo di DPIA può riguardare una singola operazione di trattamento dei dati. Tuttavia, si potrebbe ricorrere a un singolo DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Ciò potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Oppure, un singolo DPIA potrebbe essere applicabile anche a trattamenti simili attuati da diversi titolari del trattamento dei dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile un DPIA di riferimento, attuare le misure descritte nello stesso, e fornire una giustificazione per la realizzazione di un unico DPIA.

Quando si effettua la DPIA

L'art. 35 del GDPR stabilisce che è necessario effettuare una DPIA in tutti i casi in cui le operazioni di trattamento presentano rischi elevati per i diritti e le libertà delle persone fisiche in virtù della loro natura, portata o finalità o quando possono procurare un danno economico o sociale importante.

La DPIA deve essere effettuata prima di procedere al trattamento, già dalla fase di progettazione del trattamento stesso anche se alcune delle operazioni di trattamento non sono ancora note, in coerenza con i principi di ***Privacy by design e by default*** per determinare se il trattamento deve prevedere misure opportune in grado di mitigare i rischi.

L'aggiornamento della DPIA nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità

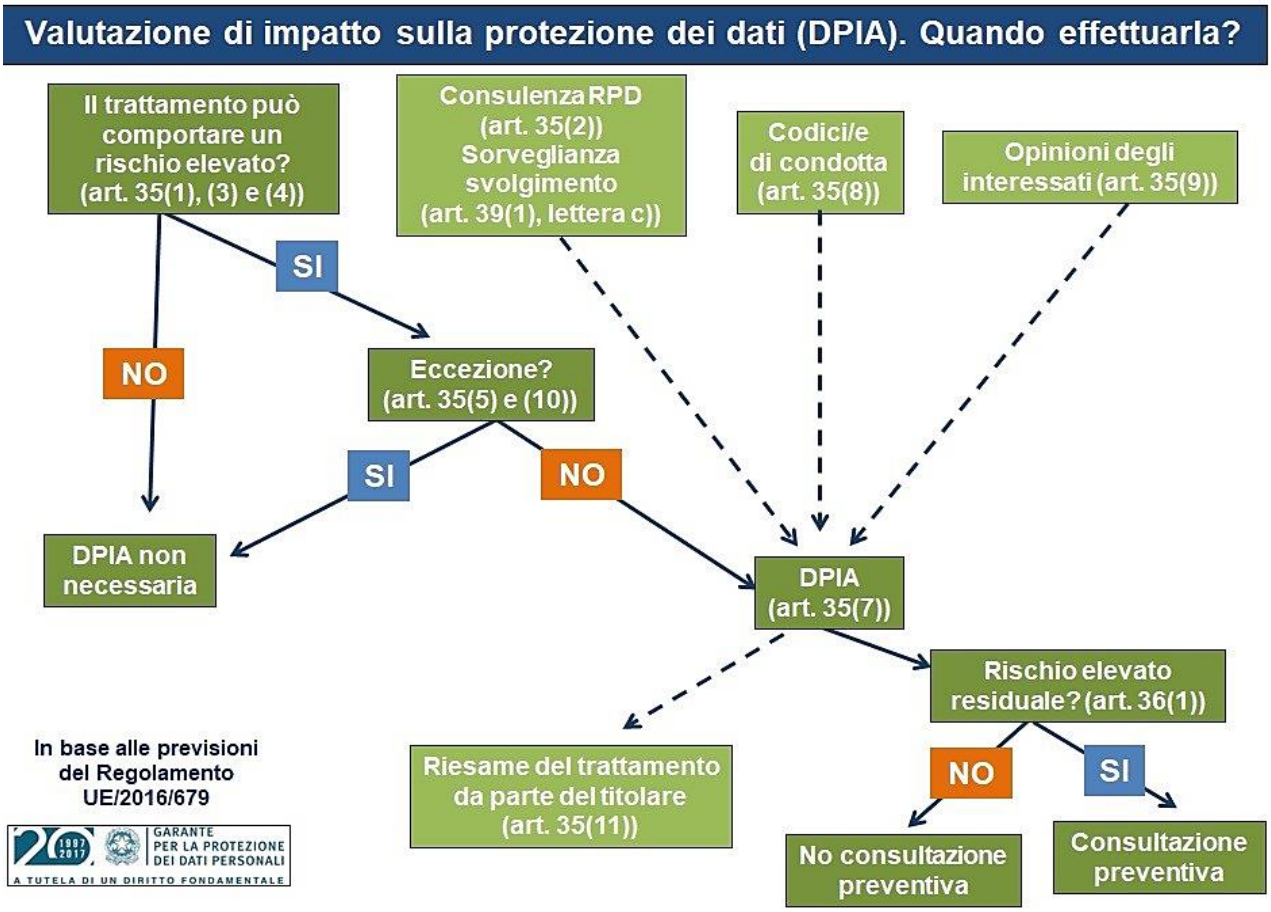
La DPIA concorre quindi, insieme ad eventuali altri processi di valutazione e gestione del rischio alla "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" come previsto dall'art. 25.

Ciò consente di acquisire le necessarie conoscenze sulle misure, garanzie e meccanismi da prevedere per mitigare il rischio e assicurare la conformità del trattamento al GDPR, prima che possano essere arrecati danni ai diritti ed alle libertà delle persone fisiche.

Al fine di garantire la corretta attivazione di un processo di DPIA è bene definire alcuni punti di attenzione in cui valutare appunto la necessità di realizzare o meno un Privacy Impact Assessment:

- Introduzione di nuovi trattamenti nell'ambito di nuovi processi e/o nuove attività;
- Importanti revisioni del modello organizzativo, con effetti su processi e relativi trattamenti;
- Nuovi servizi informativi e/o modifica dei servizi informatici in essere a supporto di trattamenti esistenti;
- Variazioni significative a Trattamenti in essere.

Di seguito lo schema (fonte Garante per la protezione dei dati personali) che chiarisce il processo di valutazione della obbligatorietà di un processo DPIA, e tutti gli elementi che ne concorrono.



Quando è obbligatorio effettuare un DPIA

La realizzazione di una DPIA è obbligatoria soltanto qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1, 3 e 4).

Sebbene una DPIA possa essere richiesta anche in altre circostanze, l'articolo 35, paragrafo 3, fornisce alcuni esempi, non esaustivi, di casi nei quali un trattamento "possa presentare rischi elevati":

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche12;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".

Vi possono essere trattamenti a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati e sui quali è necessario effettuare una DPIA.

La linea guida WP248 offre alcuni spunti e criteri di valutazione da tenere in considerazione al fine di valutare la necessità o meno di effettuare una DPIA di un trattamento. Le indicazioni prevedono che nel caso in cui un trattamento ricada in **almeno due delle seguenti categorie** si renda necessario lo sviluppo di un processo di valutazione di impatto:

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"

2. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche";

3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico";

4. dati sensibili o dati aventi carattere altamente personale: questo criterio include

categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10.

5. trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento;

6. creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;

7. dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a causa dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti.

8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc.;

9. quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.

In alcuni casi, un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una valutazione d'impatto sulla protezione dei dati.

Nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, si raccomanda di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati.

Quando è possibile NON effettuare un DPIA

Una valutazione d'impatto sulla protezione dei dati non è richiesta nei seguenti casi:

- quando il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1);
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 11);
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10), a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;
- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5).

I contenuti della DPIA

L'art. 35 al paragrafo 7 definisce il contenuto minimo che deve comunque essere assicurato per la redazione di un DPIA:

- "una descrizione dei trattamenti previsti e delle finalità del trattamento";
- "una valutazione della necessità e proporzionalità dei trattamenti";
- "una valutazione dei rischi per i diritti e le libertà degli interessati";
- "le misure previste per:
  - "affrontare i rischi";
  - "dimostrare la conformità al presente regolamento".

Partendo dai punti offerti dal paragrafo 7 ed integrandoli con i suggerimenti offerti dalle line guida WP248 si propone uno schema di massima per la realizzazione di una DPIA conforme alle prescrizioni del GDPR:

1. la descrizione sistematica del trattamento e delle finalità;
2. la descrizione della natura, dell'ambito, del contesto e degli scopi del trattamento;
3. i dati personali trattati, i destinatari e il periodo per il quale sono conservati;
4. una descrizione funzionale dell'operazione di trattamento;
5. la descrizione dell'asset model su cui si basano i dati personali (es. Siti, hardware, software, reti, organizzazione, ecc.);
6. la valutazione della necessità e la proporzionalità del trattamento;
7. la descrizione delle misure previste per conformarsi al regolamento;
8. la descrizione del modo in cui sono gestiti i rischi per i diritti e le libertà degli interessati;
9. la descrizione dell'origine, della natura, della particolarità e della gravità dei rischi;
10. la determinazione delle misure previste per il trattamento di tali rischi;
11. la descrizione del modo in cui sono coinvolte le parti interessate;
12. il parere del DPO;
13. le opinioni eventualmente raccolte dagli interessati o dei loro rappresentanti.

DPIA e Analisi dei rischi

Metodologia di analisi dei rischi nella DPIA

Uno degli aspetti più rilevanti nella realizzazione di un'analisi dei rischi è fissare fin da subito una metodologia definita, condivisa e ripetibile in grado di accompagnare il Titolare in un processo ricorsivo da ripetersi con cadenza puntuale o al cambiare del contesto di riferimento. Spesso l'elemento più rilevante di un'analisi dei rischi non è tanto il valore assoluto dei suoi risultati, in termini spesso "qualitativi", ma è il confronto dei risultati rispetto alla precedente "elaborazione" che deve far comprendere all'azienda il trend di miglioramento in corso. Lo scopo è sempre quello di ridurre al minimo, per quanto possibile, i rischi con una corretta valutazione e successiva gestione.

L'analisi del rischio è quindi un processo per identificare e valutare il danno causabile da minacce e vulnerabilità in combinazione su uno o più Asset aziendali ben precisi. Serve inoltre a giustificare le contromisure, a valutare che siano efficaci, di costo ragionevole, effettivamente applicabili al contesto e in grado di rispondere in tempo alle minacce.

Permette anche di assegnare una priorità di trattamento dei rischi e consentire di determinare l'investimento necessario all'azienda per proteggersi da essi.

Gli obiettivi principali dell'analisi del rischio sono:

- Identificarlo
- Quantificare l'impatto
- Permettere di individuare il bilanciamento ottimale tra l'impatto e il costo delle misure di sicurezza necessarie a ridurlo

È quindi una funzione che vede la possibilità di subire perdite al seguito del verificarsi di un evento dannoso rappresentabile con la seguente funzione: **R = f (I/G, P, V)**

Dove **R** (***il rischio***) è funzione delle vulnerabilità e degli ***Impatti/Gravità*** (**I/G**) e ***Probabilità*** (**P**) delle possibili Minacce che possono insistere sulle vulnerabilità.

L'analisi dei rischi, in estrema sintesi, si sostanzia nelle risposte alle seguenti domande:

- ℜ Quali sono i miei asset da proteggere e qual' è il loro valore? (i dati e i trattamenti)
- ℜ Cosa potrebbe accadere? (qual è la minaccia e su quale vulnerabilità può insistere?)
- ℜ Quale danno potrebbe causare (qual è l'impatto sui diritti dell'interessato?)
- ℜ Quanto spesso può accadere? (qual è la frequenza di accadimento?)

Risulta quindi chiaro che uno dei primi elementi da identificare in una analisi dei rischi è il dominio degli asset su cui intervenire e il loro valore. Solo una corretta valorizzazione ci consente di sviluppare una corretta analisi dei rischi arrivando a contromisure che siano in linea ed adeguate al valore dell'asset da proteggere.

Applicando quanto espresso sopra al contesto di un'analisi dei rischi in ambito DPIA è evidente che tale analisi ha come obiettivo minimizzare la probabilità e impatti che possibili violazioni dei dati personali potrebbe comportare agli individui (distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato ai dati).

Per ciò che riguarda invece il valore alla base delle analisi dei rischi in ambito GDPR deve essere chiaro che non si tratta del valore che l'informazione ha per il Titolare (che comunque può essere tenuto in considerazione per la valutazione di ulteriori soluzioni di sicurezza per la protezione del valore legato alla proprietà intellettuale dell'informazione) ma bensì al valore che il trattamento, e le relative informazioni in esso contenute, hanno per l'interessato.

Il GDPR offre ai Titolari del trattamento la flessibilità di stabilire la struttura e la forma precise della DPIA in maniera da consentire che la stessa si adatti alle pratiche esistenti.

STRUMENTI A SUPPORTO DI UN PROCESSO DPIA

Un esempio di un **software applicativo** per la gestione di un processo DPIA è "PIA", scaricabile gratuitamente dal sito di **CNIL** (Autorità francese per la protezione dei dati).

Il software, al quale ha aderito anche il Garante Italiano, non costituisce un modello obbligatorio, ma offre un focus sugli elementi di cui si compone la procedura di DPIA. Costituisce quindi un supporto metodologico allo svolgimento di una DPIA.

Integrazione dell'analisi dei rischi DPIA con l'analisi dei rischi

Il GDPR fa riferimento all'obbligo del titolare (ed eventualmente del responsabile) di tenere conto dei rischi che i trattamenti possono comportare per i diritti e le libertà delle persone fisiche in due norme diverse:

- l'art.24 e 25, collocano l'analisi dei rischi fra le caratteristiche dei trattamenti di cui occorre tener conto per mettere in atto tutte le misure tecniche e organizzative adeguate
- l'art. 35, che prevede invece una specifica valutazione di impatto quando i trattamenti, considerate le circostanze indicate nella norma, possono presentare rischi elevati per gli interessati.

Anche dalla lettura della WP248 emerge che, in base all'art. 24, ogni trattamento deve essere analizzato dal titolare anche al fine di verificare se i rischi che ne derivano siano o no elevati. Ne consegue che anche l'analisi implicitamente prevista dall'art.24 è finalizzata all'accertamento del livello di rischio perché solo a valle di questa il titolare può decidere se il rischio per i cittadini sia elevato o meno.

In questo senso, come sottolinea il WP248, prima di porre in essere un qualunque trattamento, è sempre necessaria l'analisi dei rischi che possono derivarne.

La differenza tra le misure di sicurezza da adottare per via di quanto previsto dagli art. 24 e 25 e quelle che devono essere adottate per via di quanto previsto dall' art. 35 emerge solo a valle della analisi preventiva dei trattamenti, ed è sulla base di questa che il titolare dovrà decidere in concreto quali misure adottare.

Quanto espresso quindi dagli art.24 e 25 può essere riconducibile al concetto di Privacy by default, applicabile quindi a tutti i trattamenti a prescindere dalla loro potenziale criticità derivante dal trattamento di informazioni che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Ne deriva che è sempre necessaria un'analisi dei rischi di "base" in grado di garantire una sicurezza minima e una conformità sulle modalità di trattamento su tutti i trattamenti in essere.

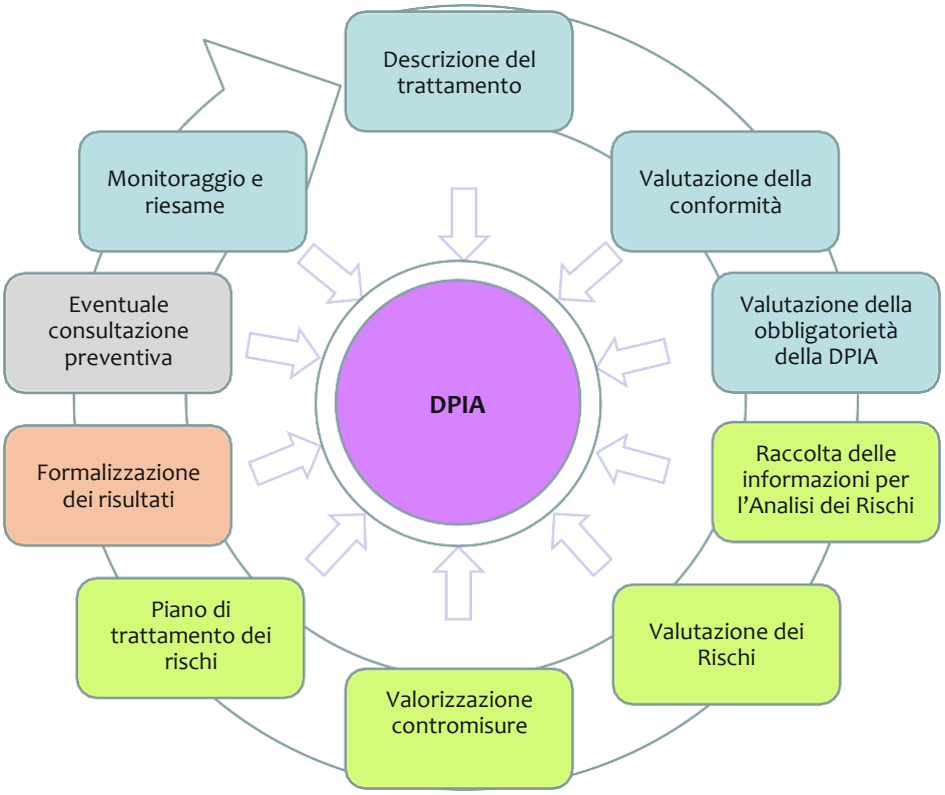
PROCESSO DPIA

Il processo DPIA

Un processo DPIA (normalmente) si compone di **5 fasi principali**:

1. Valutazione preliminare: scopo dell'attività è quella di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento è conforme al regolamento GDPR e in seconda battura comprendere se quel trattamento deve essere sottoposto ad una valutazione DPIA. L'attività quindi si scompone di 3 sotto fasi:
   a. Descrizione del trattamento
   b. Valutazione della conformità
   c. Valutazione della obbligatorietà di condurre una DPIA
2. Esecuzione DPIA: una volta determinata la necessità di procedere ad una attività di DPIA si rende necessario procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti. L'attività si scompone in ulteriori 4 sotto fasi:
   a. Raccolta delle informazioni per l'analisi dei rischi
   b. Valutazione dei rischi
   c. Valorizzazione contromisure e rischio residuo
   d. Piano di trattamento dei rischi
3. Formalizzazione dei risultati: valutare se le misure individuate sono idonee a mitigare i rischi ad un livello accettabile, stimando in tal senso un rischio residuo, nonché documentare i risultati di tutte le attività svolte durante la DPIA ed i razionali che determinano la scelta se procedere o meno alla Consultazione Preventiva
4. Consultazione Preventiva(Eventuale): consultare l'Autorità di Controllo qualora non sia stato possibile ridurre il rischio residuo a un livello accettabile. L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.
5. Monitoraggio e Riesame: il processo DPIA è riconducibile al ciclo di Denim, dove le attività una volta terminate devono prevedere un monitoraggio dei risultati raggiunti e un conseguente riesame costante al fine di garantire nel tempo la mitigazione dei rischi e la conformità al GDPR anche a fronte di fisiologici cambiamenti a cui sono soggetti tutti i trattamenti (contesto interno e esterno, finalità del trattamento, strumenti utilizzati, organizzazione, ecc.)

Di seguito uno schema riassuntivo dei principali passaggi previsti da un processo DPIA



Valutazione preliminare

Raccolta delle informazioni per la valutazione preliminare

In questa fase devono essere fornite le informazioni rilevanti ai fini del censimento del trattamento stesso e per la valutazione dei rischi, tra cui sinteticamente:

- le categorie di soggetti interessati dal trattamento;
- le finalità del trattamento;
- le categorie di dati oggetto del trattamento;
- le modalità di trattamento;
- il luogo / i luoghi di conservazione dei dati trattati;
- i processi aziendali che saranno coinvolti nell'attuazione del trattamento

La responsabilità per il censimento e la raccolta delle informazioni relative al trattamento è in capo al responsabile del processo (Designato/Delegato) a cui afferisce il potenziale trattamento, coadiuvato dal Referente interno e dal DPO.

Un ulteriore dettaglio dei dati da raccogliere è possibile trovarlo nel Registro dei trattamenti.

Valutazione della conformità

Una volta raccolte tutte le informazioni utili a identificare e censire il trattamento, si rende necessaria, come prima attività, l'analisi della necessità e della proporzionalità del trattamento rispetto alle finalità, con lo scopo di rendere espliciti gli scopi di impiego dei dati perseguiti con il trattamento e le ragioni delle modalità adottate e gli interessi legittimi del Titolare.

Il Referente interno, avvalendosi se necessario del supporto del DPO, verifica che vi siano tutti i presupposti per effettuare un trattamento conforme ai requisiti GDPR. La responsabilità per la corretta esecuzione delle verifiche preventive rimane comunque in carico al Designato/Delegato.

Si dovranno verificare almeno i seguenti aspetti:

- il trattamento rispetta i princìpi applicabili al trattamento dei dati personali:
  - principio di liceità, correttezza e trasparenza;
  - principio di limitazione della finalità;
  - principio di minimizzazione dei dati;
  - principio di esattezza dei dati;
  - principio di limitazione della conservazione dei dati;
  - principio di integrità e riservatezza.
- il trattamento rispetta i diritti degli interessati:
  - diritto di informazione;
  - diritto di accesso ai dati;
  - diritto di portabilità dei dati;
  - diritto di rettifica dei dati;
  - diritto di cancellazione dei dati ("diritto all'oblio");
  - diritto di limitazione del trattamento;
  - diritto di opposizione al trattamento.

Qualora tutte le verifiche portino ad un esisto positivo il trattamento è conforme e si può procedere ad effettuare la valutazione successiva (Valutazione dell'obbligo/esenzione DPIA). Qualora invece le verifiche portino ad un esito negativo il trattamento non può essere effettuato, almeno con le finalità, modalità e mezzi previsti all'interno dell'analisi appena effettuata.

Valutazione dell'obbligo/esenzione DPIA

Il DPO, con l'ausilio operativo del Designato/Delegato e del Referente interno, ha successivamente l'onere di verificare se il trattamento ricade nella casistica di quelli che necessitano obbligatoriamente di una valutazione di impatto (DPIA)

Il DPO, insieme al Referente interno e al Designato/Delegato, verificheranno principalmente che:

- il trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (Art.35, par. 1);
- il trattamento ricade in una delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati (Art.35, par. 5);
- il trattamento risulta già normato di diritto (Art.35, par. 10).

Qualora la verifica porti ad un esito positivo, ovvero alla consapevolezza che si rende necessario procedere alla realizzazione del DPIA, allora si potrà procedere allo sviluppo.

Nel caso invece in cui tale obbligatorietà non esista, è consigliato (non obbligatorio) che l'esito negativo (DPIA non necessaria) sia documentato nel Registro dei trattamenti e/o nel documento di analisi dei rischi.

Esecuzione DPIA

<u>Raccolta delle informazioni per l'analisi dei rischi</u>

L'analisi dei rischi DPIA si basa su una raccolta di informazioni in grado di caratterizzare il trattamento e le sue peculiarità, ovvero raccogliere alcune informazioni fra cui:

- Informazioni presenti all'interno dei trattamenti
- Processi aziendali su cui insistono i trattamenti
- Finalità dei dati raccolti
- Flussi informativi
- Autorizzati all'accesso alle informazioni
- Asset model a sostegno dei trattamenti (applicativi, hardware, reti, ecc.)

Tali informazioni si possono raccogliere o all'interno dell'organizzazione o da documentazione esistente e/o interviste oppure ricavandole da quanto raccolto durante la fase di Audit.

Le valutazioni che dovranno essere fatte durante la fase di analisi dei rischi devono tenere in considerazione due aspetti fondamentali: sia i rischi derivanti dai contenuti intrinseci

del trattamento stesso comprendenti soprattutto modalità e finalità sia i rischi derivanti da possibili violazioni di sicurezza della protezione del dato.

In entrambi i casi è importante identificare le minacce che insistono sui trattamenti (volontarie e/o accidentali) sempre nell'ottica della tutela dei diritti dell'interessato.

Valutazione dei rischi

La valutazione dei rischi all'interno di una DPIA è di norma sviluppata nel classico concetto di valutazione degli ***impatti/gravità*** e ***probabilità*** afferenti ad una serie di minacce (analizzate singolarmente o nel loro complesso).

Formalizzazione dei risultati

La documentazione prodotta deve concorrere alla realizzazione di un Report finale (***Documento di DPIA***) in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal GDPR.

**La valutazione complessiva di impatto, o una sua sintesi, può essere resa pubblica da parte del titolare in un'ottica di trasparenza nei confronti degli interessati. Contenuti e modalità dell'eventuale pubblicazione può essere concordata con il DPO.*

Il Report deve inoltre esplicitare la frequenza di aggiornamento del DPIA.

Consultazione preventiva

Qualora la Valutazione d'Impatto sulla protezione dei dati a cui si è giunti al termine del processo DPIA e riportato all'interno del Report conclusivo, indichi che il trattamento possa presentare un rischio elevato in assenza di misure adottabili dal Titolare del trattamento in grado di attenuare il rischio, il Titolare del trattamento (o suo delegato), prima di procedere al trattamento, deve consultare l'Autorità di Controllo. Tale adempimento deve essere considerato parte integrante del processo di DPIA.

Quando è necessaria la consultazione preventiva

La consultazione preventiva all'autorità garante è quindi sostanzialmente obbligatoria in due casi:

- Ogni qualvolta il Titolare non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati)
- Qualora il diritto dello Stato membro in questione prescriva che i Titolari consultino l'autorità di controllo e/o ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (articolo 36, par. 5).

Contenuti della consultazione preventiva

La responsabilità dell'attivazione della Consultazione preventiva è responsabilità del DPO, su delega del Titolare, in accordo con i Designati/Delegati (o Referente interno) a cui fa riferimento il trattamento oggetto della DPIA.

La consultazione preventiva, deve contenere alcune informazioni fondamentali fra cui:

a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le finalità e i mezzi del trattamento previsto;

c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;

d) ove applicabile, i dati di contatto del titolare della protezione dei dati;

e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;

f) ogni altra informazione richiesta dall'autorità di controllo.

*****Nella richiesta di Consultazione Preventiva devono inoltre essere indicati i dati di contatto del DPO.

Salvo diversa disposizione dell'Autorità garante è bene che la comunicazione di Richiesta di Consultazione avvenga con modalità che consentano di dimostrare la data certa della stessa comunicazione (es. PEC, Raccomandata, ecc.) visto che i tempi stabiliti per lo sviluppo del processo di consultazione preventiva decorreranno da tal data.

Processo della consultazione preventiva

Quando è stata richiesta una valutazione preventiva all'Autorità di Controllo, il trattamento **non può essere iniziato** almeno fino a che in procedimento di consultazione preventiva si è concluso con successo. L'autorità a questo punto ha 8 settimane, prorogabili una sola volta di altre 6 settimane, per concludere la consultazione. Nel caso in cui non dovesse pervenire alcuna risposta entro il termine di otto settimane, il **silenzio assenso** dell'Autorità potrà quindi essere interpretato come una **implicita conferma**.

Se invece l'Autorità ha ravvisato una possibile violazione del regolamento in quanto per il trattamento in questione il Titolare non abbia identificato o attenuato il rischio, la medesima potrà fornire un parere scritto al Titolare del trattamento in tal senso.

Nel caso in cui invece il trattamento venga ritenuto particolarmente complesso da esaminare e richieda più tempo l'Autorità potrà richiedere, entro un mese dal ricevimento della richiesta di Consultazione, una proroga di ulteriori sei settimane (solo per una volta).

Revisione del processo DPIA

La DPIA non è da intendersi come un'attività puntuale da effettuarsi una tantum, ma è un processo che deve essere ***ciclicamente attuato e revisionato*** tutte le volte che si rende necessario in base ai cambiamenti interni o esterni che si dovessero presentare al trattamento.

Anche la linea guida WP248 sottolinea la necessità di effettuare la DPIA ad intervalli periodici, con una frequenza almeno triennale, anche se non dovessero sopraggiungere cambiamenti apparenti al trattamento. *Nel caso di modifiche a trattamenti esistenti si deve prevedere sempre una revisione della DPIA.

A seguire alcuni esempi di modifiche alle attività di trattamento, rischi connessi e cambiamenti nel contesto organizzativo o sociale che debbono indurre ad una revisione:

- Cambiamento sulle attività di trattamento, in termini di:
  - Contesto
  - Finalità del trattamento,
  - Tipologia di dati personali trattati
  - Destinatari
  - Modalità di raccolta dei dati personali
  - Combinazioni di dati provenienti da fonti differenti
  - Trasferimento di dati all'estero
- Modifica ai rischi con impatto sui diritti degli interessati derivati da:
  - Presenza di nuove minacce
  - Modifica ai sistemi informativi a supporto del trattamento
  - Soppressione di contromisure esistenti
  - Nuovi scenari di rischio
  - Nuovi potenziali impatti/gravità sulle dimensioni di analisi
  - Attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali.

Inoltre, si rende comunque necessaria una revisione della DPIA tutte le volte che si è in presenza di mutamenti nel contesto organizzativo o sociale per il trattamento in essere.

ASPETTI SANZIONATORI

Violazioni

Con il termine violazioni si fa riferimento a quelle irregolarità nella gestione del processo di DPIA che possono essere oggetto di sanzione a seguito di controllo delle autorità di controllo individuate.

Sanzioni

La mancata esecuzione di una DPIA nei casi in cui il trattamento è soggetto alla stessa (articolo 35, paragrafi 1, 3 e 4), o la mancata consultazione dell'autorità di controllo laddove richiesto (articolo 36, paragrafo 3, lettera e)), può comportare una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di EUR oppure, nel caso di un'impresa, pari a fino al 2% del fatturato annuo globale dell'anno precedente, a seconda di quale dei due importi sia quello superiore.

ALLEGATI

- Verifica preliminare applicabilità DPIA
- Richiesta parere DPIA
- Comunicazione aggiornamenti su DPIA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 4 ottobre 2017

Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?

È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGPD**) che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione *(accountability)* in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.** Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti**, e **non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** *(Chief Information Security Officer, CISO)* e **del responsabile IT**.

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/regolamentoue